Mutually unbiased weighing matrices and a two-fold cover of strongly regular graphs (Research on finite groups and their representations, vertex operator algebras, and algebraic combinatorics)

AUTHOR(S):

須田, 庄

数理解析研究所講究録
第1965巻 2015年 129-134

Mutually unbiased weighing matrices and a two-fold cover of strongly regular graphs

愛知教育大　須田庄 (Sho Suda)
Aichi University of Education

1 序

Mutually unbiased weighing matrices は mutually unbiased bases の一般化した概念である. Mutually unbiased bases とあるアソシエーションスキームの存在性は Q-多項式スキームの研究で重要な定理である [9, Theorems 4.1,4.2]. 本稿では mutually unbiased weighing matrices から得られるアソシエーションスキームについて論じたい. Mutually unbiased bases の場合とは対照的に任意の mutually unbiased weighing matrices からはアソシエーションスキームは得られないが, アソシエーションスキームが付随するときには強正則グラフの spread との関連があり非常に興味深い. 考えている空間は実球面であるが, 同様の議論を複素球面に拡張することもできる. 本稿の最後に Rudvalis 群と関係する複素格子から得られるアソシエーションスキームについても触れる.

2 Mutually unbiased weighing matrices

W を成分を $0, \pm 1$ とする d 次の正方行列とする. W が重さ k の weighing matrix であるとは, $WW^T = kI$ を満たすこととする. ここで, I は単位行列とする. 定義から明らかなように $k = d$ となる weighing matrix は位数 d の Hadamard matrix に一致する.

Mutually unbiased weighing matrices の定義は Holzmann, Kharaghani, Orrick によって次のように与えられている [7]. 位数 d, 重さ k の weighing matrices W_1, W_2 が unbiased であるとは, $\frac{1}{\sqrt{k}} H_1 H_2^T$ が重さ k の weighing matrix になることとし, mutually unbiased weighing matrices とは重さ k の weighing matrices $W_1, \ldots, W_f$ であって, 任意の相異なる i, j に対して W_i, W_j が unbiased であることとする. 重さが位数と等しい mutually unbiased weighing matrices は mutually unbiased Hadamard matrices と呼ばれており, 本質的に mutually unbiased bases と同値な概念である.

Mutually unbiased weighing matrices の興味深い例は次で与えられる.

Example 2.1. E_8 root system の 240 個のベクトルは, 15 個の 2-frame $\mathcal{B}_1, \ldots, \mathcal{B}_{15}$ で分割される. ここで 2-frame とは $\langle f_i, f_j \rangle = 0$ $(1 \leq i < j \leq 8)$ を満たす長さが 2 のベクトルからなる集合 $\{\pm f_1, \ldots, \pm f_8\}$ のことである. 2-frame $\mathcal{B}_1$ を正規直交基底の $\sqrt{2}$ 倍したものになるように E_8 root system を直交変換で移す. E_8 root system の相異なるベクトルの内積は

$\pm 1, 0, -2$ であるので, $\mathcal{B}_1$ との内積を考えることで $\mathcal{B}_2, \ldots, \mathcal{B}_{15}$ の各 frame を構成するベクトルの成分は $\pm 1/\sqrt{2}, 0$ となる. 各 $\mathcal{B}_i$ $(i = 2, \ldots, 15)$ の極対的なベクトル (-1 倍で移りあうベクトル) から一方を選び, それらを行ベクトルとする行列を $\sqrt{2}$ 倍したものを W_i とする. このとき, W_i $(i = 2, \ldots, 15)$ は重さが 4 の mutually unbiased weighing matrices となっている.

3 Association schemes

Mutually unbiased weighing matrices を単に球面上の有限集合とみなし, 内積を二項関係とするアソシエーションスキームはいつ付随するか、という問題を考える.

X を有限集合, R_i $(i = 0, \ldots, n)$ を X 上の空でない二項関係とする. 各 R_i に対して, R_i の隣接行列 A_i を次で定める:

$$(A_i)_{xy} = \begin{cases} 1 & ((x, y) \in R_i \text{ のとき}) \\ 0 & (\text{その他}) \end{cases}$$

$(X, \{R_i\}_{i=0}^n)$ が可換アソシエーションスキームであるとは次の条件を満たすときとする:

(1) A_0 は単位行列.

(2) $\sum_{i=0}^n A_i = J$ (J はすべての成分が 1 の正方行列である).

(3) 任意の $i \in \{0, 1, \ldots, n\}$ に対して, $A_i^T \in \{A_1, \ldots, A_n\}$ (A_i^T は A_i の転置行列である).

(4) 任意の $i, j, k \in \{0, 1, \ldots, n\}$ に対して, ある非負整数 $p_{i,j}^k$ が存在して, 次が成り立つ; $A_i A_j = \sum_{k=0}^n p_{i,j}^k A_k$.

すべての $i \in \{1, \ldots, n\}$ に対して A_i が対称行列のとき, $(X, \{R_i\}_{i=0}^n)$ を対称という。本稿ではアソシエーションスキームといえば対称なものを意味することとする.

位数 d, 重さ k の mutually unbiased weighing matrices $W_1, \ldots, W_f$ から d 次元の実球面 S^{d-1} 上の有限集合 X を以下のようにして作る. X_i を W_i $(i = 1, \ldots, f)$ の正規化した行ベクトルおよびその -1 倍したベクトルからなる $2d$ 点の有限集合とし, $X = \bigcup_{i=1}^f X_i$ とする. X の内積集合 $A(X) := \{\langle x, y \rangle \mid x, y \in X, x \neq y\}$ は $A(X) = \{\pm \frac{1}{\sqrt{k}}, 0, -1\}$ で与えられる. $\alpha_0 = 1, \alpha_1 = -1, \alpha_2 = \frac{1}{\sqrt{k}}, \alpha_3 = \frac{-1}{\sqrt{k}}, \alpha_4 = 0$ とおく. 内積から X 上の二項関係を次のように定める:

$$R_i = \{(x, y) \in X \times X \mid \langle x, y \rangle = \alpha_i\} \qquad (i = 0, 1, \ldots, 4).$$

また, X_i に現れる内積 0 と, X_i と X_j $(i \neq j)$ に現れる内積 0 の役割が異なるので, 更に $\tilde{R}_i$ を次のように定義する:

$$\begin{aligned} \tilde{R}_i &= R_i \text{ for } i \in \{0, 1, 2, 3\}, \\ \tilde{R}_4 &= R_4 \cap \bigcup_{i \neq j} (X_i \times X_j), \\ \tilde{R}_5 &= R_4 \setminus \tilde{R}_4. \end{aligned}$$

一般に $(X, \{R_i\}_{i=0}^4)$, $(X, \{\tilde{R}_i\}_{i=0}^5)$ 共にアソシエーションスキームにならないが, 次の定理が成り立つ.

Theorem 3.1. もし $(X, \{R_i\}_{i=0}^4)$ がアソシエーションスキームであれば, $(X, \{\tilde{R}_i\}_{i=0}^5)$ もアソシエーションスキームになる.

E_8 root system の 240 個のベクトルは内積を二項関係として, クラスが 4 のアソシエーションスキームになることはよく知られている. 上記の定理を用いることにより, E_8 root system の 2-frame 分解がクラス 5 のアソシエーションスキームを導くことがわかる.

Theorem 3.1 は球面上のデザイン議論を用いて証明することもできるが, より一般の定理を次の章で紹介し, その際に本質的な役割を果たす強正則グラフの spread について紹介する.

4 Spreads in strongly regular graphs

グラフ $G = (V, E)$ とは, 有限集合 V と V の 2 点部分集合全体のなす集合の部分集合 E がなす組のことである.

パラメーター (v, k, λ, μ) の強正則グラフ (strongly regular graph) とは, 頂点数が v, 各頂点に隣接している頂点の個数が k であり, 相異なる勝手な二頂点 x, y に隣接している頂点の個数は x, y が隣接しているか否かに応じて λ, μ となるグラフのことである. グラフの隣接行列とは, G の頂点集合で添え字づけられた正方行列で

$$A_{xy} = \begin{cases} 1 & (x, y \text{ が隣接しているとき}) \\ 0 & (\text{その他}) \end{cases}$$

と定める.

グラフ $G = (V, E)$ のクリークとは, どの 2 頂点も隣接している V の部分集合のことである. 強正則グラフのクリークに含まれる頂点の最大数はグラフの隣接行列の固有値を用いて次のように評価できる. ここで, k-正則グラフの隣接行列の最大固有値は k であることに注意しておく.

Theorem 4.1 (Delsarete bound). $G = (V, E)$ を強正則グラフとし, C を G のクリークとする. A の最小固有値を θ とする. このとき, $|C| \leq 1 - k/\theta$ が成り立つ.

強正則グラフのクリークで Theorem 4.1 の等号が成立するものを Delsarte クリークと呼ぶ. 頂点集合が Delsarte クリークにより分解されている状況を考察する [4, 6].

Definition 4.2. 強正則グラフの spread とは, Delsarte クリークからなる集合 $\{C_1, \ldots, C_f\}$ で頂点集合を分割しているものである.

これは partial geometry の spread に由来する概念である [3].

強正則グラフは定義からクラスが 2 のアソシエーションスキームであるが, もしも spread が存在するとクラスが 3 のアソシエーションスキームが構成できる.

Theorem 4.3. ([4, Theorem], [6, Proposition 4.1]) $G=(V,E)$ を強正則グラフ, $\{C_1,\dots,C_f\}$ を G の *spread* とする. 頂点集合 V 上の二項関係を次のように定める:

$$\begin{aligned}R_0&=\{(x,x)\mid x\in V\},\\ R_1&=\{(x,y)\mid \{x,y\}\in E,\{x,y\}\in\cup_{i=1}^{f}C_i\},\\ R_2&=\{(x,y)\mid \{x,y\}\in E,\{x,y\}\notin\cup_{i=1}^{f}C_i\},\\ R_3&=\{(x,y)\mid \{x,y\}\notin E\}.\end{aligned}$$

このとき, $(V,\{R_i\}_{i=0}^3)$ はアソシエーションスキームとなる.

Remark 4.4. Theorem 4.3 の記号において, $(V,\{R_0,R_1\cup R_2,R_3\})$ はクラスが 2 のアソシエーションスキームである. 逆にクラスが 2 のアソシエーションスキームがあれば R_0 でない二項関係を辺集合とするグラフは強正則グラフとなる.

$(X,\{R_i\}_{i=0}^4)$ をアソシエーションスキームとし, R_4 の次数を 1 を仮定する. このとき, $R_0\cup R_4$ は X 上の同値関係をなし, また隣接行列の添え字集合 $\{0,1,\dots,4\}$ 上の同値関係を次により定める: $i,j\in\{0,1,\dots,4\}$ に対して $i\sim j\Leftrightarrow$ ある $\alpha\in\{0,4\}$ が存在して $p_{i,\alpha}^{j}\neq 0$. この同値関係による同値類を $\{0,4\},\{1,3\},\{2\}$ となるように添え字を付け直す. 二項関係 R_4 の次数が 1 であるので, 次の性質を満たす X 上の全単射 ϕ が存在する: 任意の $x\in X$ に対して, $(x,\phi(x))\in R_4$. このとき適当に頂点集合を並び替えることで, ある $(0,1)$-行列 $\overline{A}_0,\overline{A}_1,\overline{A}_2$ が存在して次が成り立つ:

$$A_0+A_4=\overline{A}_0\otimes J_2,\quad A_1+A_3=\overline{A}_1\otimes J_2,\quad A_2=\overline{A}_2\otimes J_2.$$

このとき [1, Theorem 9.3] により, $\overline{A}_0,\overline{A}_1,\overline{A}_2$ はクラス 2 のアソシエーションスキームの隣接行列となる. クラスが 2 のアソシエーションスキームを $(\overline{X},\{\overline{R}_i\}_{i=0}^2)$ とすると, $\overline{X}$ は $(x,y)\in R_4$ となる X の二頂点 x,y を同一視している. この同一視を商写像とよび $\psi:X\to\overline{X}$ と書くことにする.

クラスが 2 のアソシエーションスキームは強正則グラフなので, $(X,\{R_i\}_{i=0}^4)$ を強正則グラフの two-fold cover とよぶ.

上記の通り定義されたアソシエーションスキーム $(X,\{R_i\}_{i=0}^4)$ に対して, X の部分集合 Y が $\{0,2,4\}$-クリークであるとは $\{i\mid R_i\cap(Y\times Y)\neq\emptyset\}=\{0,2,4\}$ が成り立つときとする. これは Y の相異なる二頂点は R_2 もしくは R_4 で結ばれていることを意味している. Y の商写像による像は $\overline{R}_2$ を辺集合とする強正則グラフのクリークである.

Theorem 3.1 の定理はより一般に次の形で定式化される.

Theorem 4.5. ([11, Theorem 3.2]) $(X,\{R_i\}_{i=0}^4)$ を強正則グラフの *two-fold cover* とする. $Y_1,\dots,Y_f$ を $\{0,2,4\}$-クリークとし, $\{Y_1,\dots,Y_f\}$ は X の分割を与えるとする. もし $\psi(Y_i)$ $(i=1,\dots,f)$ が強正則グラフ $(\overline{X},\overline{R}_2)$ の *Delsarte* クリークであれば, $(X,\{\tilde{R}_i\}_{i=0}^5)$ はアソシエーションスキームである. ただし $\tilde{R}_i$ は次で定義される:

$$\begin{aligned}\tilde{R}_i&=R_i\ \textit{for}\ i=0,1,3,4,\\ \tilde{R}_2&=R_2\cap\bigcup_{i=1}^{f}(Y_i\times Y_i),\\ \tilde{R}_5&=R_2\setminus\tilde{R}_2.\end{aligned}$$

Example 4.6. E_8 root system の極対的な 2 点を同一視し, 内積 0 で辺を結んだグラフはパラメーター $(120, 63, 30, 36)$ の強正則グラフ G となる. このグラフの次数, 最小固有値はそれぞれ $63, -9$ であるので Theorem 4.1 の Delsarte bound は $1 - 63/(-9) = 8$ となる. したがって各 2-frame は商グラフ G において Delsatre クリークとなる. よって E_8 root system の 2-frame 分解は商グラフ G において Delsatre クリークによる頂点集合の分割, すなわち spread となる. この spread により Theorem 4.3 からクラスが 3 のアソシエーションスキームが得られる.

E_8 root system はクラスが 4 のアソシエーションスキームとなり, パラメーター $(120, 63, 30, 36)$ の強正則グラフの two-fold cover である. Theorem 4.5 を E_8 root system の 2-frame 分解に用いるとクラスが 5 のアソシエーションスキームが得られる.

5 今後の展望

同様の現象を複素球面上のアソシエーションスキームに対して考察していくことは興味深い. このような試みは, Best[2] により定義を複素数にまで拡張させた weighing matrix の unbiased な例の構成が行われており, それらは可換アソシエーションスキームになっている例が少なくない. これから特に次の例に対して考察できたら非常に興味深いと思われる.

Rudvalis 群は 28 次元のある複素格子 L の自己同型群として得られる. その複素格子 L は 16240 個の minimum vector を持ち, minimum vector からなる集合を X とおく. このとき次が知られている:

Proposition 5.1. ([5, Lemma 9], [8, 命題 6.2]) $A(X) := \{\langle x, y\rangle \mid x, y \in X, x \neq y\} = \{0, \pm 1, \pm i, -4, \pm 4i\}$.

Proposition 5.2. ([5, Theorem 2], [8, 命題 6.3]) $\pm 1, \pm i$ 倍で移りあう X の点を同一視した点を頂点とし, 内積 0 で辺集合を作るとパラメーター $(4060, 1755, 730, 780)$ の強正則グラフが得られる.

Problem 5.3. *Proposition 5.2* の強正則グラフに *spread* は存在するか.

このグラフの最大固有値, 最小固有値はそれぞれ $1755, -65$ であるので, Delsarte bound は $1 - 1755/(-65) = 28$ となる (複素格子 L の次元と一致する). $4060/28 = 145$ となるので, 頂点集合を互いに交わりのない 145 個の 28 点のクリークに分解できるか, という問題と同値である.

これが肯定的に分かると, 次の二つのことが得られる.

- Theorem 4.3 によりクラスが 3 のアソシエーションスキームが得られる.
- Propositions 5.1,5.2, [10, Lemma 3.2] を用いると, X は 28 次元の複素球面の $\mathcal{T}$-design となる. ここで $\mathcal{T} = \{(k, l) \in \mathbb{Z}^2 \mid 0 \leq k, l \leq 3\} \setminus \{(3, 3)\}$ である. さらに [10, Theorem 8.1(ii)] を用いると X は内積を二項関係としてクラスが 8 の可換アソシエーションスキームとなることがわかる. X が 4-frame 分解できたとすると, 内積 0 の二項関係を同じ frame に属している二頂点か否かで二つの二項関係に分けるとことでクラスが 9 の可換アソシエーションスキームが得られる.

参考文献

[1] E. Bannai, T. Ito, Algebraic Combinatorics I: Association Schemes, Benjamin/Cummings, Menro Park, CA, 1984.

[2] D. Best, Biangular vecors, Master thesis, Lethbrdge Unibersity, 2014.

[3] R. C. Bose, Strongly regular graphs, partial geometries and partially balanced designs, *Pacific J. Math.* **13** (1963), no. 2, 389–419.

[4] Y. Chang, Imprimitive Symmetric Association Schemes of Rank 4, Ph-D Thesis, University of Michigan, 1994.

[5] 千吉良直紀, Rudvalis 群と格子, 第 57 回代数学シンポジウム報告集, 2012.

[6] W. H. Haemers and V. D. Tonchev, Spreads in strongly regular graphs, *Des. Codes and Crypt.*, **8** (1996), 145–157.

[7] W. H. Holzmann, H. Kharaghani and W. Orrick, On the real unbiased Hadamard matrices, *Combinatorics and graphs*, 243–250, Contemp. Math., 531, Amer. Math. Soc., Providence, RI, 2010.

[8] 北詰正顕, Rudvalis 群に対する複素格子について, RIMS 講究録 1811「有限群とその表現, 頂点作用素代数, 組合せ論の研究」2012 年 3 月.

[9] N. LeCompte, W. J. Martin, W. Owens, On the equivalence between real mutually unbiased bases and a certain class of association schemes, *European J. Combin.* **31** (2010), no. 6, 1499–1512.

[10] A. Roy and S. Suda, complex spherical designs and codes, *J. Combin. Des.* **22** (2014), 105–148.

[11] S. Suda, A two-fold cover of strongly regular graphs with spreads and association schemes of class five, *Des. Codes and Crypt.*, to appear.